



Использование сетевой телеметрии для охоты на угрозы

или как увидеть то, о чем мы не знаем?

Руслан Иванов

Старший инженер по информационной безопасности

ruivanov@cisco.com

Неизвестная зона

Не известно аналитику

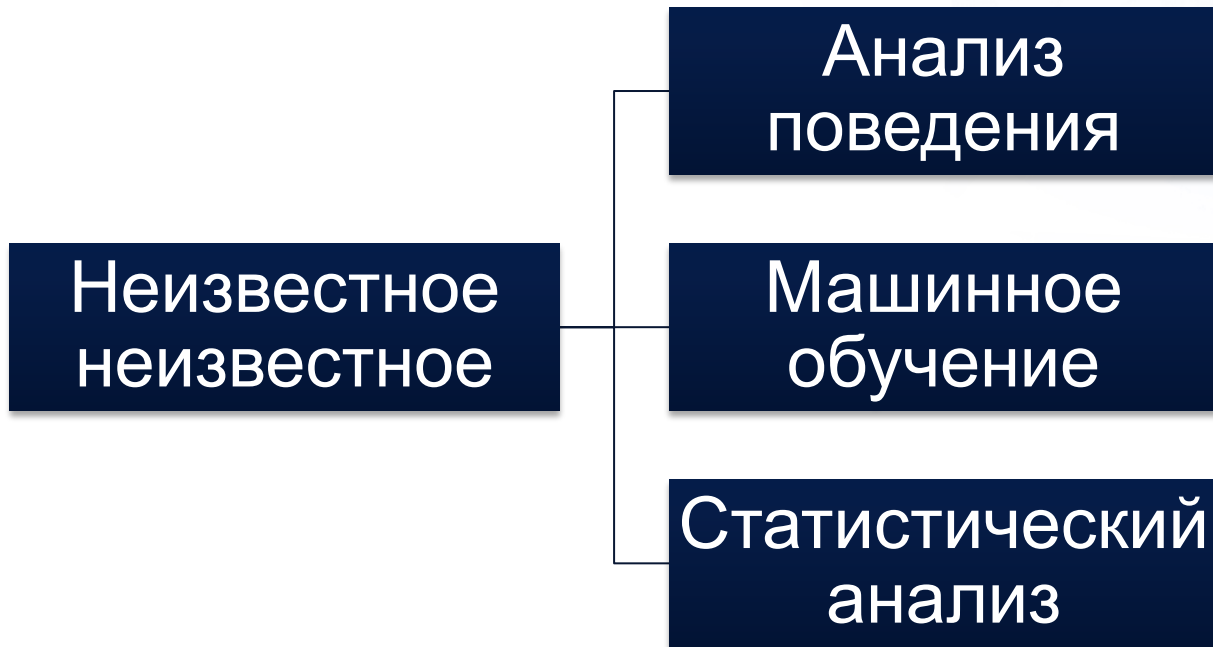
Не
известно
другим

Выпадающие события / «Черный лебедь»
Аномальное поведение
0-Days
Еще нет сигнатур/решающих правил

События типа «чёрный лебедь»

«В России такого никогда не было и вот опять повторилось» В. С. Черномырдин

Обнаружение угроз в неизвестной зоне



Обнаружение аномалий и классификация событий

Обнаружение аномалий

- Скажи мне если произойдет что-то необычное

Классификация

- Скажи мне когда ты увидишь нечто, похожее на это

Вспомним распечатку мобильного оператора



Day	Date	Time	To/From	Type	Msg/KB/Min	Rate Code	Rate PD	Feature	In/Out
TUE	07/17/14	9:43AM	571492	CALL	13 Min	TM1	AT	SMH	Out
TUE	07/10/14	8:10PM	293538	TXT	5Msg	TM1	AT	SMH	Out
WED	07/11/14	7:33AM	349737	TXT	20Msg	TM1	AT	SMH	In
WED	07/11/14	12:12PM	345787	CALL	190 Min	TM1	AT	SMH	In
WED	07/11/14	2:15PM	985687	CALL	43 Min	TM1	AT	SMH	In
THR	07/12/14	5:23AM	345784	TXT	5Msg	TM1	AT	SMH	Out
THR	07/12/14	6:17AM	293538	CALL	58 Min	TM1	AT	SMH	Out
FRI	07/13/14	10:57AM	349737	TXT	5Msg	TM1	AT	SMH	In
FRI	07/13/14	1:57PM	935693	TXT	13Msg	TM1	AT	SMH	Out
FRI	07/13/14	8:37PM	985687	TXT	9Msg	TM1	AT	SMH	In
MON	07/16/14	11:41PM	293538	CALL	14 Min	TM1	AT	SMH	In
TUE	07/17/14	4:20PM	472091	TXT	7Msg	TM1	AT	SMH	Out
TUE	07/17/14	9:27AM	293538	CALL	8 Min	TM1	AT	SMH	In
TUE	07/17/14	9:43AM	571492	CALL	13 Min	TM1	AT	SMH	Out

Вспомним распечатку мобильного оператора



Day	Date	Time	To/From	Type	Msg/KB/Min	Rate Code	Rate PD	Feature	In/Out
TUE	07/17/14	9:43AM	571492	CALL	13 Min	TM1	AT	SMH	Out
TUE	07/10/14	8:10PM	293538	TXT	5Msg	TM1	AT	SMH	Out
WED	07/11/14	7:33AM	349737	TXT	20Msg	TM1	AT	SMH	In
WED	07/11/14	12:12PM	345787	CALL	190 Min	TM1	AT	SMH	In
WED	07/11/14	2:15PM	985687	CALL	43 Min	TM1	AT	SMH	In
THR	07/12/14	5:23AM	345784	TXT	5Msg	TM1	AT	SMH	Out
THR	07/12/14	6:17AM	293538	CALL	58 Min	TM1	AT	SMH	Out
FRI	07/13/14	10:57AM	349737	TXT	5Msg	TM1	AT	SMH	In
FRI	07/13/14	1:57PM	935693	TXT	13Msg	TM1	AT	SMH	Out
FRI	07/13/14	8:37PM	985687	TXT	9Msg	TM1	AT	SMH	In
MON	07/16/14	11:41PM	293538	CALL	14 Min	TM1	AT	SMH	In
TUE	07/17/14	4:20PM	472091	TXT	7Msg	TM1	AT	SMH	Out
TUE	07/17/14	9:27AM	293538	CALL	8 Min	TM1	AT	SMH	In
TUE	07/17/14	9:43AM	571492	CALL	13 Min	TM1	AT	SMH	Out

Анализ сетевой телеметрии Netflow (jFlow, sFlow) – путь к самообучаемым сетям



Мощный источник информации для каждого сетевого соединения

Каждое сетевое соединения
в течение длительного интервала времени
IP-адрес источника и назначения, IP-порты,
время, дата передачи и другое
Сохранено для будущего анализа



Важный инструмент для идентификации взломов

Идентификация аномальной активности
Реконструкция последовательности событий
Соответствие требованиям и сбор доказательств
NetFlow для полных деталей, NetFlow-Lite для 1/n
семплов

NetFlow с точки зрения контекста

Кто

Start: 06/12 - 06:49:19 AM
End: 06/12 - 06:51:20 AM
Duration: 2m 1s

10.201.3.78
RFC 1918
ethel
14:7d:c5:bf:31:85
[View Details](#)

Откуда

Что

60173/TCP

Как

11.72KB | 63 packets
80/TCP

→
HTTP
←

30.53KB | 45 packets

Куда

184.75.210.3
Canada

Когда

Больше контекста

Flow Detailed Summary: 10.201.3.78

Search Subject Details	Totals	Peer Details
Packets: 63	Packets: 108	Packets: 45
Packet Rate: 0.52pps	Packet Rate: 0.89pps	Packet Rate: 0.37pps
Bytes: 11.72KB	Bytes: 42.24KB	Bytes: 30.53KB
Byte Rate: 99.15bps	Byte Rate: 357.48bps	Byte Rate: 258.33bps
Percent Transfer: 27.7%	Search Subject/Peer Ratio: 0.38	Percent Transfer: 72.3%
Host Groups: Sales and Marketing, End User Devices, Atlanta	TCP Connections: 12	Host Groups: Canada
Payload: GET http://www.acronymfinder.com/~/stl/digg.gif	RTT: 70ms	Payload: 200 OK
	SRT: 4ms	

Высокомасштабируемый сбор
Высокое сжатие => долговременное хранилище

CISCO

Close

С помощью NetFlow можно обнаруживать не столько известные угрозы, сколько аномалии

Стадия атаки

Обнаружение

1

Использование уязвимостей

Злоумышленник сканирует IP-адреса и порты для поиска уязвимостей (ОС, пользователи, приложения)

- NetFlow может обнаружить сканирование диапазонов IP
- NetFlow может обнаружить сканирование портов на каждом IP-адресе

2

Установка вредоносного ПО на первый узел

Хакер устанавливает ПО для получения доступа

- NetFlow может обнаружить входящий управляющий трафик с неожиданного месторасположения

3

Соединение с “Command and Control”

Вредоносное ПО создает соединение с C&C серверами для получения инструкций

- NetFlow может обнаружить исходящий трафик к известным адресам серверов C&C

4

Распространение вредоносного ПО на другие узлы

Атака других систем в сети через использование уязвимостей

- NetFlow может обнаружить сканирование диапазонов IP
- NetFlow может обнаружить сканирование портов на каждом IP-адресе внутреннего узла

5

Утечка данных

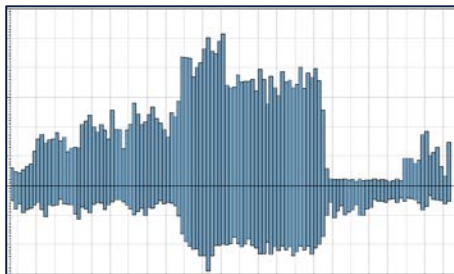
Отправка данных на внешние сервера

- NetFlow может обнаружить расширенные потоки (HTTP, FTP, GETMAIL, MAPIGET и другие) и передачу данных на внешние узлы

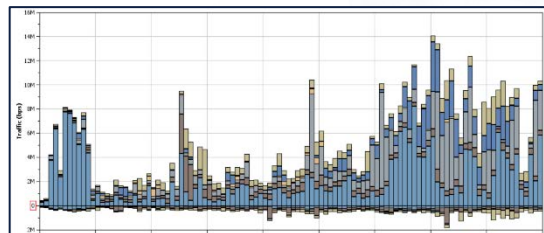


Сетевое обнаружение аномалий (NBAD)

- Отчёты по группам хостов выдают сетевые шаблоны и шаблоны приложений



Inbound/Outbound
Отчет по трафику



Отчет по приложениям



- Concern Index** отслеживает хосты компрометирующие сеть

New York, Desktops	10.50.100.83	190,075,544	1,901%	High Concern Index, High File Sharing Index, High Total Traffic	Ping, Rejects, TCP_Scan
--------------------	--------------	-------------	--------	---	-------------------------

- File Sharing Index** показывает активность пиринговых сессий

Atlanta, Trusted Wireless	10.10.200.59	180,385	361%	High Concern Index, High File Sharing Index, High Total Traffic	Ping, Ping_Scan, Port_Scan, TCP_Scan, TCP_Stealth
---------------------------	--------------	---------	------	---	---

- Target Index** показывает хосты являющиеся жертвами вредоносной активности

Domain Controllers, Atlanta, DNS Servers, NTP Servers	10.10.30.15	118,019,003	11,802%		Excess_Clients, Rejects
---	-------------	-------------	---------	--	-------------------------

StealthWatch – внутренние нарушители и угрозы

- **Неавторизованный доступ:** попытка нарушения политик, блокирована на МСЭ

vernon	Denied	10.203.0.202	QA, Windows, Chicago, PCI Unauthorized	Engineering, PCI Unauthorized	30s	HTTPS (unclassified)
--------	--------	--------------	--	-------------------------------	-----	----------------------

- **Внутреннее обследование:** *Concern Index* событие , сканирование на порту tcp/445

Apr 17, 2013 12:39:57 AM (22 hours 7 minutes 4s ago)	Apr 17, 2013 10:40:06 PM (6 minutes 55s ago)	Atlanta, Engineer	10.202.0.0/24	5,576,380	Addr_Scan/tcp-445(11380)
---	---	-------------------	---------------	-----------	--------------------------

- **Утечка данных:** идентификация подозрительной передачи данных через Интернет-периметр в течение длительного времени

		Desktops & Trusted Wireless	Apr 15, 2013 4:20:00 PM (7 minutes 7s ago)	Suspect Data Loss	10.10.101.89	Desktops, Atlanta	ud0158	Multiple Hosts	Observed 1.87G bytes. Policy maximum allows up to 500M bytes.
--	--	--	---	-------------------	--------------	-------------------	--------	----------------	--

- **Накопление данных:** передача больших объемов данных через сеть
 - **Подозрение на накопление данных** – хост загружает данные со многих других хостов
 - **Таргетированный вывод данных**– Хост выкачивает большой объем данных через множество других хостов

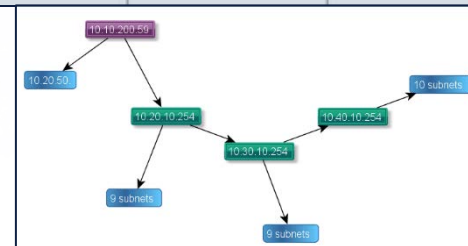
Target Data Hoarding	<input checked="" type="checkbox"/>	<input type="checkbox"/>	None	Tolerance: 92 Never trigger alarm when less than: 500M downloaded payload bytes in 24 hours Always trigger alarm when greater than: 1T downloaded payload bytes in 24 hours	None
----------------------	-------------------------------------	--------------------------	------	---	------

Обработка Индикаторов компрометации (IoCs)


- Идентификация подозреваемых в заражении **Malware хостов** в группах клиентских машин

10.50.100.83	POS Terminals	199.188.204.182	United States	38s	FTP	2.2k
--------------	---------------	-----------------	---------------	-----	-----	------

- Визуализация распространения заражения Malware с помощью **Worm Tracker**
 - **Основные и вторичные** заражения
 - **Сканируемые** подсети



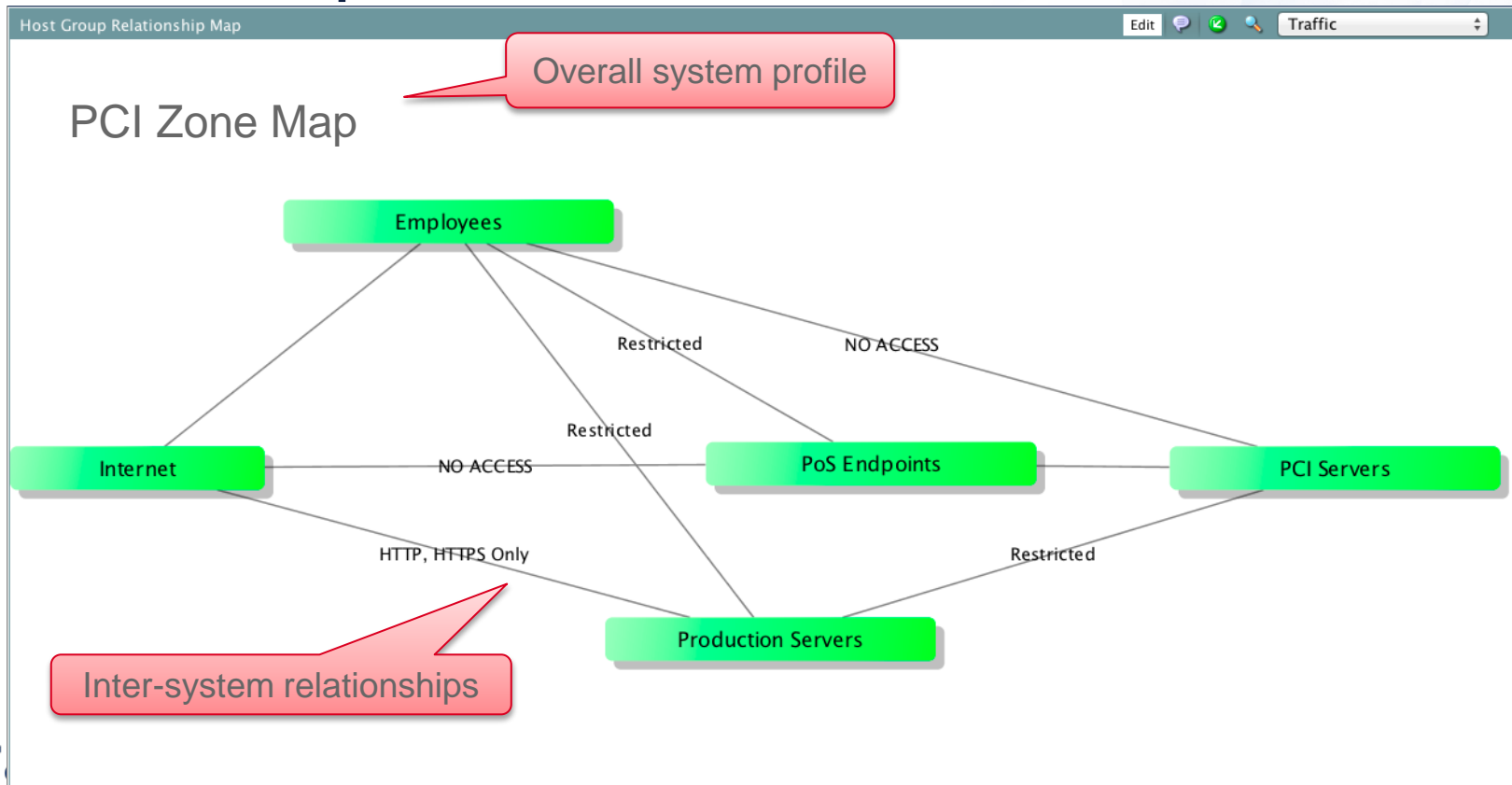
- Применение контекстно-насыщенной телеметрии от **ISE** для понимания вовлеченных пользователей

	Jun 10, 2013 11:27:37 PM (8 days 20 hours 26 minutes ago)	Current	bmcMahon	00:d0:b8:0d:fd:27 (Iomega Corporation)	Windows7-Workstation	LC	Unknown Exporter (10.10.1.1)	GigabitEthernet5/37	
---	--	---------	----------	---	----------------------	----	---------------------------------	---------------------	--

- Узнать все ли **хосты затронуло** изначальным **заражение**

Apr 15, 2013 12:53:21 PM (11 hours 58 minutes 40s ago)	Apr 15, 2013 10:07:36 PM (2 hours 44 minutes 25s ago)	Atlanta, Trusted Wireless	10.10.200.59	Domain Controllers, Atlanta, DNS Servers, NTP Servers	10.10.30.17
Apr 15, 2013 9:49:26 AM (15 hours 2 minutes 35s ago)	Apr 15, 2013 9:57:19 PM (2 hours 54 minutes 42s ago)	Atlanta, Trusted Wireless	10.10.200.59	Atlanta, File Servers	10.10.31.33

Моделирование и контроль Business Critical процессов в StealthWatch



Мы можем отправить хост на карантин с помощью StealthWatch

Success
Quarantine request successfully sent to ISE. To view the current quarantine status of the host, you must go to the Cisco ISE device or contact your ISE administrator.

Host Report for 10.10.18.102

Concern Index: 0 | Target Index: 0 | Recon: 0 | Data Hoarding: 0 | Exfiltration: 0 | Policy Violation: 2

Host Summary
Host IP: 10.10.18.102
Status: Active
Hostname: w7-client-3850.cts.local
Host Groups: Catch All
Location: RFC 1918
Last Seen: 5/22/15 1:28 PM
Policies: Inside
MAC Address: 00:50:56:b4:3f:af (VMware, Inc.)

Traffic by Peer Host Group (last 12 hours)
Catch All, Multicast, Broadcast, United States, 10.10.18.102

Alarms by Type (last 7 days)
Event Count: 3 on 05/19
Legend: Employees to Development Servers (Blue), Employee to PCI Server Violation (Black), Policy (Green)

Users & Sessions

Mac Address:	Mac Vendor:	Device Type:
00:50:56:b4:3f:af	VMware Inc	Unknown
User	Start	End
employee1	5/22/15 12:51 PM	5/22/15 1:29 PM

Application Traffic

Application	Total	%	Sent	Ratio	Received	7-day Trend	24-hour Trend
ICMP	176.15KB	51.00	175.85KB		516B		

Как это выглядит на ISE (используем AdaptiveNetworkControl): Live Log

Show Live Sessions Add or Remove Columns Refresh Reset Repeat Counts Refresh Every 1 minute Show Latest 20 records

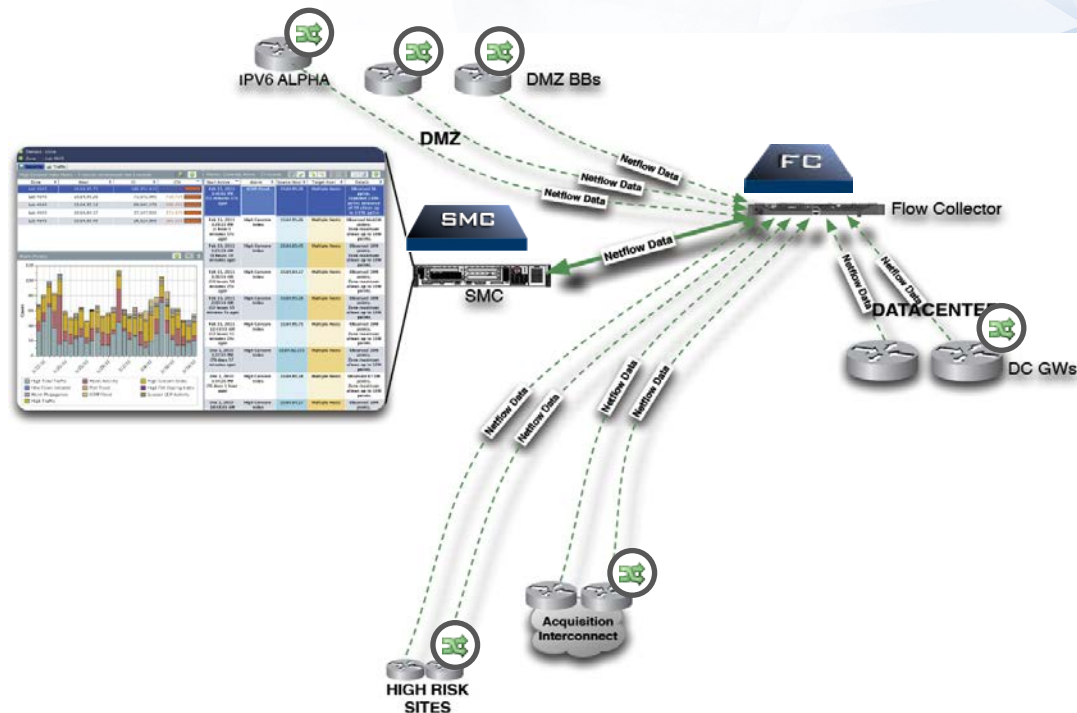
Time	Status	Details	Repeat Count	Identity	Endpoint ID	Authentication Policy	Authorization Policy	Authorization Profiles	Security Group	Network Device
2015-05-25 17:12:35.581	✓			#CTSREQUEST#					Device_SGT	N7K-DST1
2015-05-25 17:12:15.702	✓			#CTSREQUEST#					Suspicious_Investigate	N7K-DST1
2015-05-25 17:12:14.355	✓			#CTSREQUEST#					Suspicious_Investigate	cts-3850-b
2015-05-25 17:12:14.335	ⓘ			0 employee1	00:50:56:B4:3F:AF				Suspicious_Investigate	
2015-05-25 17:12:14.307	✓			employee1	00:50:56:B4:3F:AF	Default >> Dot1X >> Default	Default >> EPS Authorization Rule	Suspicious_Investigate,Per...	Suspicious_Investigate	cts-3850-b

EPStatus check

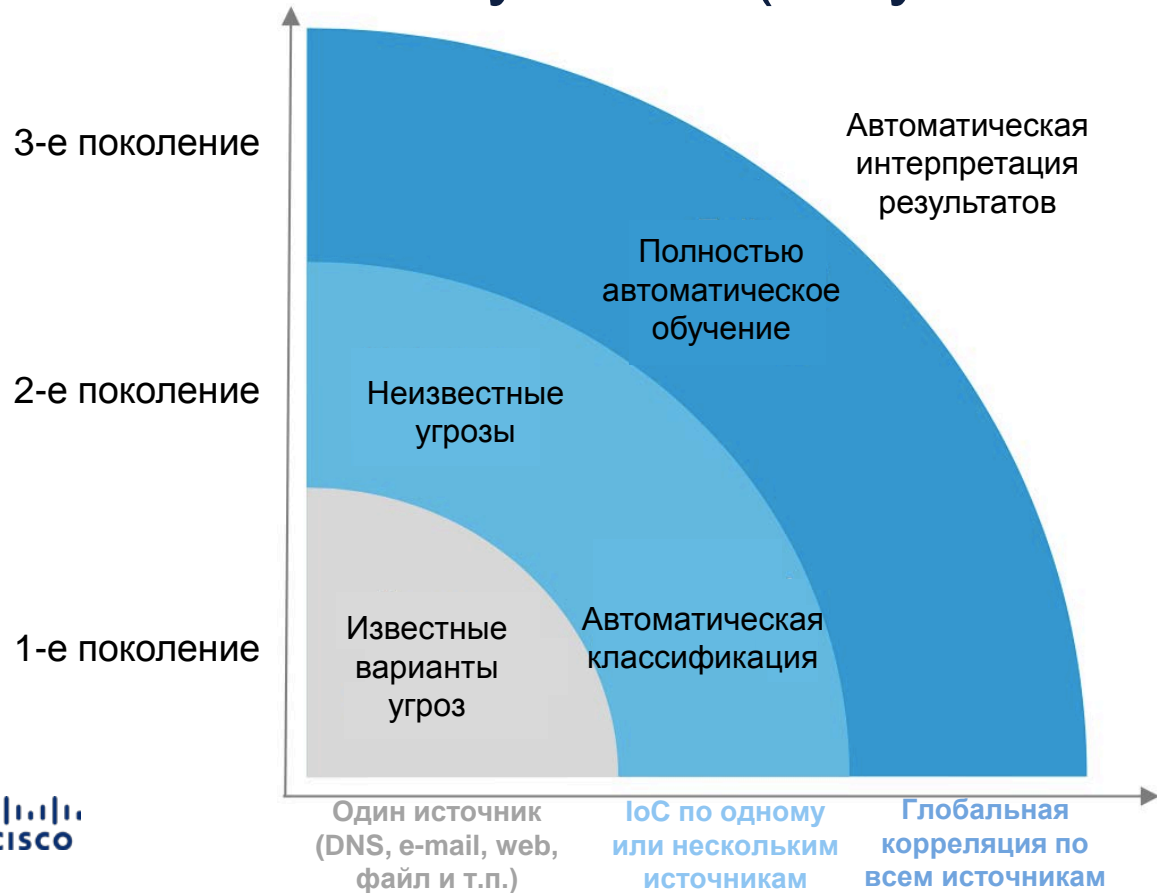
Security Group Assignment

NetFlow и StealthWatch в Cisco

- Коллекторы потоков расположены глобально
- **15 миллиардов потоков в день** в Cisco
- Cisco Stealthwatch
- Ad-hoc поиск
- Аналитика сети
- Анализ и предупреждения
 - Попытки вывода данных
 - Обмен файлами и их раздача
 - Большие объемы потоков
 - Соединения с ботнетами



Машинное обучение (искусственный интеллект)



- Машинное обучение – не панацея
- Интернет движется к тотальному шифрованию
- Злоумышленники остаются незамеченными – стеганография
- За искусственным интеллектом в ИБ – будущее

Как работает самообучающаяся сеть?

1
Обнаружение путей
прохождения трафика

1

3
Обнаружение
приложений с помощью
NBAR и DPI

3

5
Учимся отличать плохое
от хорошего

5

2
Создание карты IP-
адресов

2

4
Изучение изменений в
путях, объёмах,
шаблонов, зависимости
от времени суток

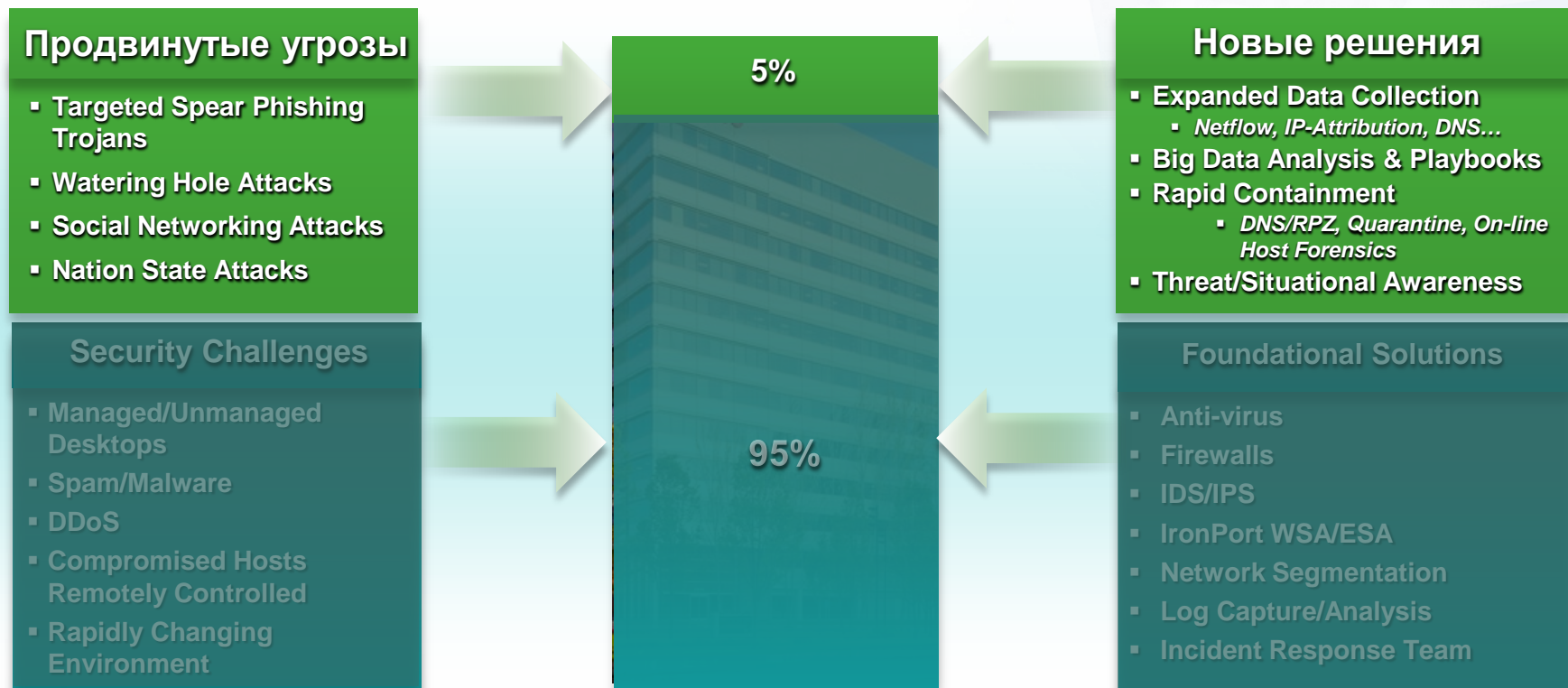
4

6
Точное обнаружение
аномалии; оператору
отправляем запрос на
реагирование

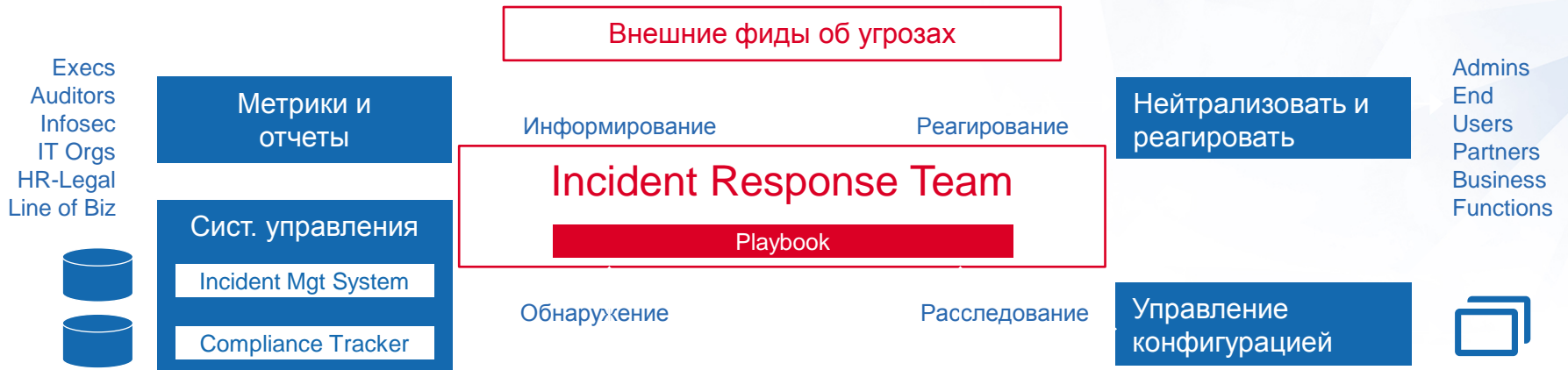
6



Не забывайте про оставшиеся 5%



Как Cisco ловит эти 5% в своей сети?



	Сканы	Конфиги	Логи	Потоки	События
Инспекция	IDS IPS NAM NetFlow Web Gateway	HIDS			
Регистрация	Syslog TACACS 802.1x Antivirus DNS DHCP NAT VPN				
Идентификация	Vuln Scans Port Scans Router Configs ARP Tables CAM Tables 802.1x				
Телеметрия	Address, Lab, Host & Employee Mgt Partner DB Host Mgt NDCS CSA, AV, Asset DB EPO, CSA Mgt, Config DB				

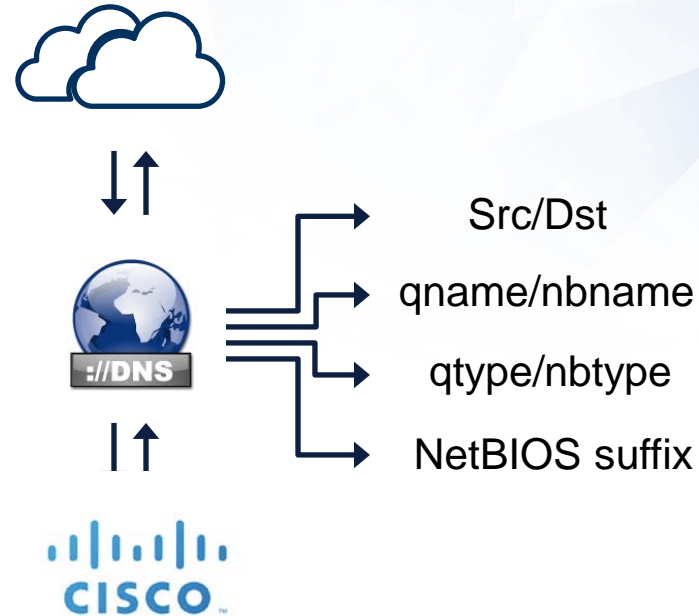
4ТВ в день

Пассивный анализ DNS @Cisco



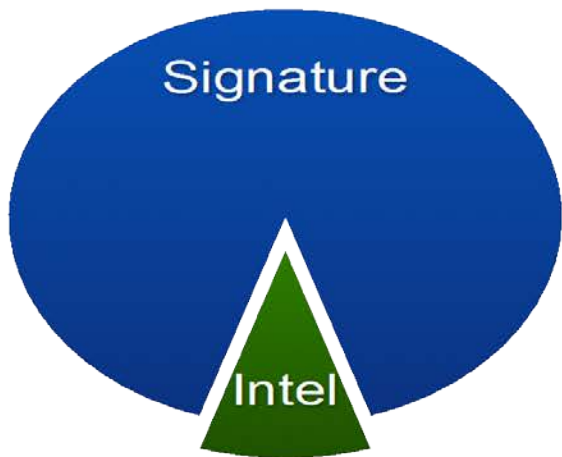
- DNS критичный сервис
- CSIRT журналирует **2.5 миллиарда DNS запросов/в день**
- Анализ DNS запросов и ответов позволяет:
 - Что пользовательская машина хочет сделать
 - Обнаружить атаки
- DNS журналы **содержат бесценную информацию**:
 - Новые домены (менее недели)
 - Fast Flux domains (много IP, короткий TTL)
 - Esoteric domains (уникальность, random generation)
 - DDNS domains
 - Ошибки резолвинга
 - Пики DNS-трафика
 - C2 сервера, забытые в вредоносы

Корреляция с NetFlow, Packet Capture и журналами приложений

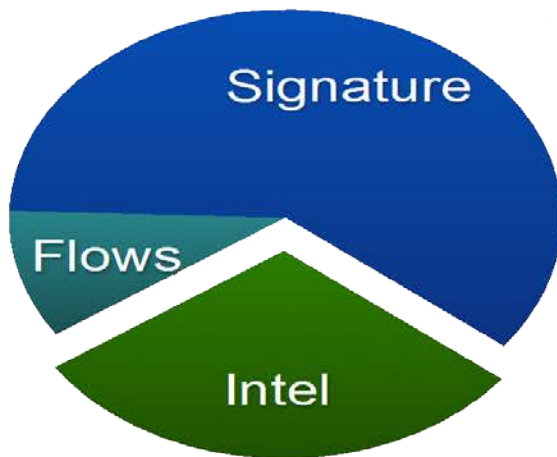


Опыт Cisco: комбинируйте методы обнаружения

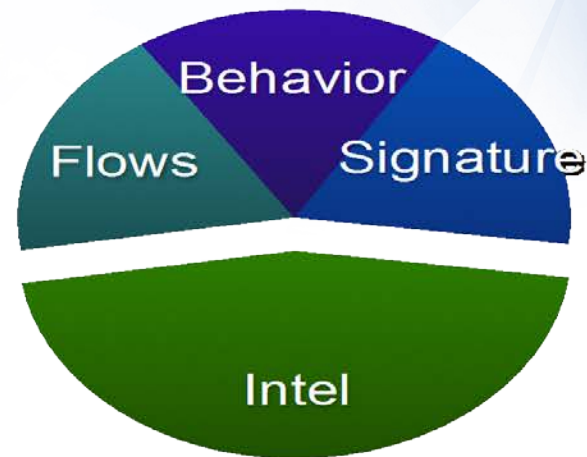
В прошлом



2012



2013+



Необходимо использовать различные способы изучения угроз
Сетевые потоки | Поведение | Сигнатуры | Исследования

Подводим итоги

Известно аналитику

Не известно аналитику

Известно
другим

Открытая

- **NGFW / NGIPS**
- **Защита от вредоносного ПО**
- **Спам-фильтры**
- **Безопасность Web**

Слепая

- **Платформы Threat Intelligence**
- **Аналитика Big data**
- **Корреляция**
- **Облачные решения**

Не
известно
другим

Скрытая

- **Визуализация**
- **Пользовательские запросы**
- **Контекст**

Неизвестная

- **Машинное обучение**
- **Статистический анализ**
- **Анализ сетевого поведения**

Интегрированная защита от угроз – это единственный путь заблокировать продвинутые угрозы

- Global Intelligence
- NGIPS & NGFW
- Identity & Access Control
- Email
- Web
- Shadow IT & Data
- DNS, IP & BGP
- Advanced Threats
- Sandboxing
- Anomaly Detection



Что сделать после семинара?

Что вам понадобится?

Выберите необходимые источники данных, обучите персонал и, по необходимости, внедрите новые решения по кибербезопасности и анализу информации для ИБ

Чего вам не хватает?

Определите ваши краткосрочные, среднесрочные и долгосрочные планы и возможные угрозы для них, а затем определите данные, которые вам нужны для их обнаружения

Что у вас есть?

Идентифицируйте используемые вами технологии ИБ, используемые данные и способы их получения, не забывая про моделирование угроз

Где вы можете узнать больше?



Пишите на security-request@cisco.com



Быть в курсе всех последних новостей вам помогут:



<http://www.facebook.com/CiscoRu>



<http://twitter.com/CiscoRussia>



<http://www.youtube.com/CiscoRussiaMedia>



<http://www.flickr.com/photos/CiscoRussia>



<http://vkontakte.ru/Cisco>



<http://blogs.cisco.ru/>



<http://habrahabr.ru/company/cisco>



<http://linkedin.com/groups/Cisco-Russia-3798428>



<http://slideshare.net/CiscoRu>



<https://plus.google.com/106603907471961036146/posts>



<http://www.cisco.ru/>

